Social Media Fostering Cybercrimes among Adults in Pakistan: Role of Lack of Empathy

Khurram Baig[1], Muhammad Salman[2], Motasem Hassan Mirza[3], Dr. Munir Ahmad[4], Dr. Abid Hussain[5], Saima Ayyaz[6]

Abstract

In criminology, digital environments are generally understood as social spaces which open new possibilities for criminal activity and crime victimization. The rapid and vast use of social media technologies has produced cybercrimes among adults. The current study was conducted to investigate the use of social media and lack of empathy as predictors of cybercrimes. The study was completed through correlational research design. Three self-administered research questionnaires were used to measure the research variables; Use of Social Media Questionnaire (SMQ), Lack of Empathy Questionnaire (LEQ), and Cybercrimes Activity Questionnaire (CAQ). Data were collected through online Google Forms. The 1191 adults provided the data. Findings of the study reveal that excessive use of social media predicts cybercrimes among adult. Moreover, results suggest that lack of empathy among adults also correlated with cybercrimes activity. In addition, both social media and lack of empathy are significant positive predictors of cybercrimes among adults. Furthermore, male adults reported greater tendency of using of social media and indulging criminal activities due to lack of empathy as compared to female adults. Role of lack of empathy is contributing a significant role in predicting cybercrimes among adults. Cybercrimes laws in Pakistan are working poorly and there is no punishment to adults who are the victim of cybercrime activities.

Keywords: Social media, lack of empathy, cybercrimes

1. Introduction

Worldwide social media usage has continued to rise. According to Chaffey (2023), 4.76 billion people, or 59% of the people worldwide, actively use social media, and the average time spent per day on social media is about two and a half hours. There was a notable increase in the amount of time spent on social media during the COVID-19 pandemic attributable to lockdown and dependence on internet services. The dangers of using social media are well documented in the research literature. Various research works have extensively discussed the security and privacy threats prevalent on social media (Yassein et al., 2019). Earlier studies focused on user identity and communication privacy concerns because of the mass sharing of personal information on social media (Zhang et al., 2010). Other privacy-related threats that arose included inference attacks, information leakage, location leakage, cyberstalking, user profiling, and surveillance (Ali et al., 2018).

Social media threats evolved with the diversity of social media features, uses, and types of shared media. Fake profiles and identity cloning sprang up for malicious purposes. The widespread use of social media for viral marketing and the installation of third-party applications led to the mass spread of malware, spamming, phishing, social engineering, and clickjacking. Cybercriminals perpetrate all these threats. (Ali et al., 2018). Fire et al. (2014) highlighted the social media crimes against children, such as predation, sharing child pornography, cyberbullying, and cyberharassment. Cybercrimes on social media can be broadly classified into cybercrimes targeting social media users, cybercrimes facilitated by social media platforms, and cybercrimes advertised on social media platforms (Umeugo, 2023).

Social media cybercrimes targeted at social media users and their accounts include privacy-violating crimes and account hijacking (Umeugo, 2023). Cybercrimes facilitated by social media are classic cybercrimes facilitated through social media. Social engineering, phishing, malware dissemination, scams, fake profiles, account impersonation, cyberstalking, spreading disinformation, spreading hate speech, and cyberharassment are examples of cybercrimes facilitated by social media (Umeugo, 2023). Cybercrimes advertised on social media platforms are illegal activities advertised on social media, such as adverts for stolen credit cards, video tutorials of unlawful acts, recruitment for illicit activities, and sharing illegally acquired intellectual property (Umeugo, 2023).

In criminology, digital environments are generally understood as social spaces which open new possibilities for criminal activity and crime victimization. Over the past decade, social media platforms have established themselves as the basic digital infrastructure that governs daily interactions. The rapid and vast adaptation of social media technologies has produced concern about the possible negative effects, but the association between social media use and decreased well-being measures appears to be rather weak (Appel et al., 2020).

2. Social Media Foster Cybercrimes

Many research studies have been done to investigate the impact of cyberbullying on victims and the part the media plays in either promoting or inhibiting it. The correlations between cyberbullying and traditional bullying were analyzed by Kowalski & Limber (2013), who also looked at how media can either encourage or discourage cyberbullying. According to the authors, encouraging young people to critically evaluate the media messages they consume can assist to reduce cyberbullying. Mesch (2009) investigated how media use can raise the risk of cyberbullying as well as the function of parental mediation in mitigating it (Tao et al., 2022). According to the author, parents who keep an eye on their kids' online activity and teach them how to use media responsibly can assist to prevent cyberbullying. The personal traits and online activities of young people who engage in online harassment were

---

[1] Ph.D. Law Scholar Gillani Law College Bahauddin Zakariya University, Multan Advocate High Court, Pakistan, mkb5729@gmail.com
[2] National Institute of Computer and Advance Studies Rahim Yar Khan, Pakistan, jamsalman818@gmail.com
[3] Department of Professional Psychology, Bahria University Lahore Campus, Pakistan, motasimmirz7@gmail.com
[4] Department of Pakistan Studies Bahauddin Zakariya University, Multan, Pakistan, munirsandhu79@gmail.com
[5] National Professional Officer, Health Department, Multan, Pakistan, drabidwho@yahoo.com
[6] Department of Professional Psychology, Bahria University Lahore Campus, Pakistan, saimaayyaz04@gmail.com

examined by Ybarra & Mitchell (2004), as well as the contribution of the media to the facilitation or prevention of cyberbullying. The authors contend that teaching young people media literacy can aid in their development of the critical thinking abilities required to fend against media messages that encourage cyberbullying. Teenagers are the biggest users of social media and the internet, according to a study from 2020 by Wuryanningsih, and Aisyah. This has an impact on the propensity for taunting in cyberbullying. Youngsters who experienced cyberbullying, whether as a bully, victim, or both, spent more time engaged in social activities while sedentary on their computers. Research have indicated that by sensationalizing the issue and fostering a climate of fear and anxiety, media coverage of cyber victimization can make matters worse. This might then result in imitation behavior and a vicious cycle of victimization. For instance, a study conducted in 2013 by Kowalski and Limber indicated that the chance of further cyberbullying occurrences in the same community increased when the incident was covered by the media.

Many research studies conclude that kids who experience bullying tend to be anxious, intimidated easily, and low on self-esteem (Cuesta et al., 2021). Cyber bullying research has also found a link between victimization and poorer levels of self-esteem, indicating that being the target of traditional bullying and becoming a victim of cyberbullying are likely related experiences (Li, & Hesketh, 2021). Moreover, victims' low self-esteem frequently causes them to be overly sensitive and incompetent in social situations and romantic relationships. Because they are frequently left alone, abandoned by other kids, and socially isolated, victims are excellent targets for bullying behavior because they lack social communication skills, are insecure about how others perceive them, and lack confidence in themselves (Özer & Escartín, 2023). Another characteristic that may both predict and be a result of bullying is anger. Cyber bullying victims may also struggle with issues like sadness and rage (Wang et al., 2020). Cyber victimization is the act of exposing a person, group, or legal entity to abusive behavior in a technological or relational context and suffering material or moral harm as a result. Individuals may suffer psychological-based grievances such as constant harassment, mockery, gossip spreading about them in the virtual environment, being exposed to insults, and spreading private photos without their consent or threatening with it, in addition to technical grievances such as the capture of their personal information and passwords as a result of virtual attacks on e-mail or websites (Merlici et al., 2022).

Researchers discovered that bullies frequently had strict, unsupportive parents (Baldry & Farrington, 2000). According to research by Wang and Ngai (2023), parental support is effective in lowering bullying and cyberbullying. A similar pattern was observed in paternal parenting techniques, with more relational hostility in kids following stricter parenting and psychologically controlling parenting methods. Teenagers who receive less parental support may therefore be more likely to engage in bullying themselves. Children who are subjected to excessive parental pressure are more likely to engage in problematic peer relationships (Maftei Măirean, 2023). Maftei Măirean, (2023), bullying and bullying tendencies have been shown to be negatively impacted by peer attachment. Peers can either escalate or stop cyber victimization, according to research. Peers who encourage, assist, or engage in harmful activity might increase cyber victimization. Additionally, they might propagate rumors or divulge sensitive information, adding to the victim's suffering. Peers can stop cyber victimization, however, by speaking out for the victim, reporting inappropriate behavior to adults, or even seeking to mediate the conflict.

According to a study by Holfeld and Grabe (2018), peers who engage in cyberbullying frequently enjoy more popularity and social standing among their peers, which may persuade other peers to follow suit. Peers who see cyber victimization taking place and step in to stop it, on the other hand, can significantly improve the victim's situation. Pozzoli et al. (2012) victims of cyberbullying experience less victimization and more feelings of social support when their peers defend them. In conclusion, peers are important in cyber victimization since they have the power to either encourage or discourage the conduct. A significant step in lowering the prevalence of cyber victimization is educating young people on how to identify and avoid becoming a victim online and promoting good actions, such as standing up for victims and confronting bullies.

3. Types of Cybercrimes

Munir and Shabir (2018), divided two categories of cybercrimes i.e. Crimes that target devices and networks and crimes that use different devices to take part in criminal activities. Major types of cybercrimes are:

3.1. Drugs Trafficking

Drug traffickers are rigorously using the internet and new media technologies to sell unlawful things through email that are encoded. Some of the drug smugglers or traffickers put the stuff on bargaining at web shopping portals, use chatting messengers and web services to sell illegal medicines, and sell or buy formulas through access to the visit rooms or chat rooms. The increment in Internet drug sales or exchanges might also be ascribed without any close or personal type of exchange of words. Such businesses do not exist in routine markets.

Electronic Money-Laundering: Electronic money exchange has started to increment aggressively so it has the potential threat that e-exchanges may be captured or interfered with. Credit card numbers are quite simply captured electronically, and physically, the computerized knowledge helped in a phenomenon that a card can be re-developed.

Hostile Content and Harassment: The data in websites and other digital means of communications may not be acceptable, foul, or against the assortment of different motives. Once in a while, such correspondences are also needed to be considered illegal. The amount of those illegal interchanges shifts heavily within the center of international locations, and even inside nations.

Dispersion of Abusive Materials: There is a huge content of cyber media that might be considered objectionable. It varies in nature such as it can be sexually abusive or explicit material, racism based, political propaganda, ethnic or religious extremist views, and much more. There are several cases in which the people post the personal pictures of their ex-boyfriends or girlfriends to create troubles in their future lives.

Digital tormenting and Cyber Stalking: Digital tormenting is taken as the usage of the Internet and other innovative gadgets to hurt others, in intentional and hostile ways. Digital tormenting may also be explained as "when internet and other electronic gadgets are utilized to disseminate the content or pictorial data to cause damage or to insult someone". Digital tormenting can be of any basic nature such as sending texts or emails to someone who doesn't want to receive your texts or messages however it can involve threats, dangers, physical or sexual assertions, harsh remarks, and publishing falsified explanations as truth.

Stealing Telecommunication: The phone pastors of the last three decades set a perspective for what has transformed into a significant crime industry of this age. Through getting to an organization's telephone switchboard, individual criminals or criminal affiliations can procure access to phone calling circuits and a while later can make their calls or offer call time to outcasts.

Piracy against Copy Rights: This type of robbery has brought on extensive worry to proprietors of the copyrighted material. "The Software Publishers Association" states that programs of billions of dollars have been stolen or pirated through the internet. Similarly, a pirated copy of the latest James Bond Film "The World is insufficient" was available free on the internet before even it was released.

Electronic Extortion and Vandalism: In no time, a western society based on industrialized colonies is connected upon complex data connection and data exchange structures. Any damage to or impedance with any of these systems can incite perilous results. Whether Different individuals and groups have hacked the site pages of various managerial and business firms. Regulatory bodies around the world are widely placing assets into information battling strategy for interfering with the information advancement and establishment of gatekeeper structures.

Digital Terrorism and Warfare: Computerized extortion is a kind of advanced terrorism in which a website, PC network, or email server is subjected by dismissing the routine administrative actions or strikes by insidious software engineers, who demand money to guarantee to stop the ambushes. While hoping such strikes might transform into the routine in future battling among nations, the thought of the web usage influences and will be balanced by fighting military heads later out of the zone.

3.2. Major Techniques of Cybercrimes
i. Botnets
ii. Cyber Stalking
iii. Malicious Software
iv. Child soliciting and Abuse
v. Ransomware
vi. Theft
vii. Identity Theft
viii. Hacking
ix. Social Engineering
x. DDoS attacks
xi. Spamming
xii. Publishing Derogatory Materials
xiii. E-Money Laundering and Taxation

3.3. Lack of Empathy as Psychological Factor of Cybercrimes
Previous studies reveal that lack of empathy predicts cybercrimes among people. Lack of empathy among adolescents and adults foster criminal activities (Kross et al., 2020). Over the last few years, the literature on the psychological, cultural, and social effects of social media has proliferated. Prior research on the topic presents a nuanced view of social media and its consequences (Kross et al., 2020). However, another line of research associates social media use with several negative effects, including higher stress levels, increased anxiety and lower self-esteem (Kross et al., 2020). Negative outcomes, such as depression, decreased subjective well-being (Wheatley & Buglass, 2019) and increased loneliness (Meshi et al., 2020), and are also commonly described in the research literature. Another study of Italian adolescents found that an individual's number of followers on Instagram was positively associated with experiences of cyber victimization (Longobardi et al., 2020). In criminology, the notion of cybercrime is used to refer to a variety of illegal activities that are performed in online networks and platforms through computers another devices (Yar & Steinmetz, 2019). As a concept, cybercrime is employed in different levels of analysis and used to describe a plethora of criminal phenomena, ranging from individual-level victimization to large-scale, society-wide operations (Donalds & Osei-Bryson, 2019). In Finland and other European countries, the most common types of cybercrime include slander, hacking, malware, online fraud, and cyberbullying.

4. Cybercrime Laws in Pakistan
As of now, there are three cybercrime laws in Pakistan. These laws deal with different categories of internet crimes in Pakistan. They are listed as under:
- Electronic Transaction Ordinance (ETO) 2002
- Electronic / Cyber Crime Bill 2007
- Prevention of Electronic Crimes Act (PECA) 2016
- Electronic Transaction Ordinance (ETO) 2002

4.1. Cybercrimes Punishments in Pakistan
Details regarding punishments for cybercrimes in Pakistan have been listed as under:

4.2. Type of Cybercrime Punishment
   i.   Data Damage: 3 years imprisonment or PKR 3 lac fine
  ii.   Electronic Fraud: 7 years imprisonment or PKR 7 lac fine
 iii.   Electronic Forgery: 7 years imprisonment or PKR 7 lac fine
 iv.   Malicious Code: 5 years imprisonment or PKR 5 lac fine
  v.   Cyberstalking: 3 years imprisonment or PKR 3 lac fine
 vi.   Spamming: 3 years imprisonment or PKR 3 lac fine
 vii.   Spoofing: 6 months imprisonment or PKR 50 thousand fine
viii.   Cyberterrorism; 10 years imprisonment or PKR 10 million fine

5. Theoretical Framework

Social Learning Theory: Bandura (1977) presented the Social Learning Theory after a series of studies proposing that people can learn from each other. They learn through observation and imitation. They also learn through modeling certain models. This learning is also based on their attention, the amount of memory engaged, and motivational factors behind that. He further suggests that human behavior is a product of different influences that include:

• Cognitive influences
 • Behavioral influences and
• Environmental influences

The theory further highlights some characteristics that help achieve effective modeling. These are:

• Attention
• Retention
• Production and
• Motivation Different aspects of Social Learning

Theory relate to the current study such as learning from the society, learning from others, learning about different kinds of cybercrimes from friends, family, social circle, and the internet itself. Awareness and learning are some important components of the current study and social learning theory fits it to a good extent. Awareness of common cybercrimes such as spoofing, hacking, phishing, tormenting, and cyber terrorism is indispensable.
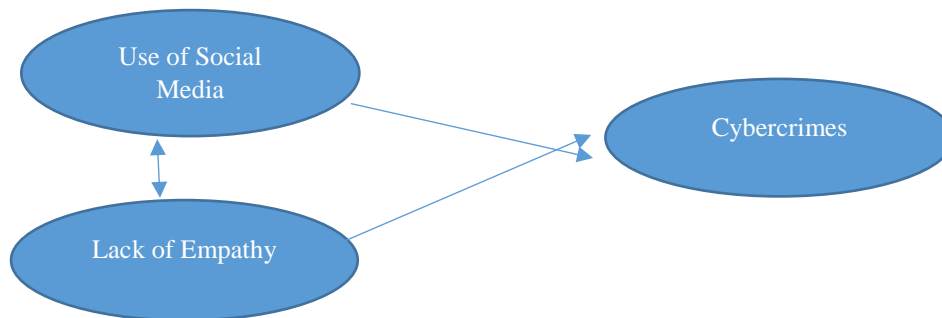
Figure 1: Conceptual Framework

Figure-1 shows the conceptual framework of the study where use of social media and lack of empathy as the predictors of cybercrimes.

5.1. Objectives of the Study
• To explore the correlation among use of social media, lack of empathy and cybercrimes
• To investigate the predictors of cybercrimes among adults
• To compare the tendency of using social media, lack of empathy and cybercrimes

5.2. Methodology

The current study was quantitative by its nature and completed through correlational research design. Google Forms survey was conducted for the purpose of data collection. Population of the study was comprised on adults. Purposive sampling techniques was employed. Sample of the study was 1191 adults among them 591 were male and 600 were females. Gender of the participants was considered as demographic variable in the study. Three self-administered research questionnaires were used to measure use of social media, lack of empathy and cybercrimes activities of adults in Pakistan. Data were analyzed on SPPS through inferential statistics by using Pearson Correlation, Multiple Regression and t-test for independent sample designs.

6. Results

eTable 1: Shows the Correlation among Using Social Media, Lack of Empathy and Cybercrimes Activities

Variables	SSM	LE	CA
Usage of Social Media	1	.732**	.835**
Lack of Empathy		1	.695**
Cybercrimes Activities			1

Correlation is significant, $p<0.05$.

Table 2: Regression Analysis showing the impact of Using Social Media and Lack of Empathy on Cybercrimes Activities

Predictor	B	Std. Error	Beta	t-test	p-value
Constant	65.34	8.132		13.231	.000
Usage of Social Media	.431	.391	. 835	11.091	.000
Lack of Empathy	.523	.432	.695	7.212	.000

Adjusted R^2 .781, $p<0.05$.

Table 3: Mean, Standard Deviation, t-value and scores of Using Social Media, Lack of Empathy and Cybercrimes Activities

Variables	Gender	N	M	Std.Deviation	Df	t-test	p-value
Social Media Usage	Male	591	14.646	32.3542	1189	11.932	.000
	Female	600	11.465	23.3321			
Lack of Empathy	Male	591	17.941	19.6475	1189	17.423	.000
	Female	600	12.253	16.5434			
Cybercrimes Activities	Male	591	23.642	25.9754	1189	21.214	.000
	Female	600	19.364	21.5497			

Difference is significant, $p<0.05$.

6.1. Discussion

In criminology, digital environments are generally understood as social spaces which open new possibilities for criminal activity and crime victimization. The rapid and vast use of social media technologies has produced cybercrimes among adults. The current study was conducted to investigate the use of social media and lack of empathy as predictors of cybercrimes. The study was completed through correlational research design. Findings of the study reveal that excessive use of social media predicts cybercrimes among adults. Social media cybercrimes targeted at social media users and their accounts include privacy-violating crimes and account hijacking (Umeugo, 2023). Cybercrimes facilitated by social media are classic cybercrimes facilitated through social media. Social engineering, phishing, malware dissemination, scams, fake profiles, account impersonation, cyberstalking, spreading disinformation, spreading hate speech, and cyberharassment are examples of cybercrimes facilitated by social media (Umeugo, 2023). Moreover, results suggest that lack of empathy among adults also correlated with cybercrimes activity. Many research studies conclude that kids who experience bullying tend to be anxious, intimidated easily, and low on self-esteem (Cuesta et al., 2021). Cyber bullying research has also found a link between victimization and poorer levels of self-esteem, indicating that being the target of traditional bullying and becoming a victim of cyberbullying are likely related experiences (Li, & Hesketh, 2021). Prior research on the topic presents a nuanced view of social media and its consequences (Kross et al., 2020). However, another line of research associates social media use with several negative effects, including higher stress levels, increased anxiety and lower self-esteem (Kross et al., 2020).

7. Conclusion

Social media's popularity and high usage make it a highly effective platform for cybercrime. Study reveal that excessive use of social media predicts cybercrimes among adult. Moreover, results suggest that lack of empathy among adults also correlated with cybercrimes activity. In addition, both social media and lack of empathy are significant positive predictors of cybercrimes among adults. Furthermore, male adults reported greater tendency of using of social media and indulging criminal activities due to lack of empathy as compared to female adults. Role of lack of empathy is contributing a significant role in predicting cybercrimes among adults. Cybercrimes laws in Pakistan are working poorly and there is no punishment to adults who are the victim of cybercrime activities.

References

Ali, S., Islam, N., Rauf, A., Din, I. U., Guizani, M., & Rodrigues, J. J. (2018). Privacy and security issues in online social networks. *Future Internet*, *10*(12), 114.

Appel, M., Marker, C., & Gnambs, T. (2020). Are social media ruining our lives? A review of meta-analytic evidence. *Review of General Psychology*, *24*(1), 60-74.

Baldry, A. C., & Farrington, D. P. (2000). Bullies and delinquents: Personal characteristics and parental styles. *Journal of community & applied social psychology*, *10*(1), 17-31

Bandura, A., & Walters, R. H. (1977). *Social learning theory* (Vol. 1). Prentice Hall: Englewood cliffs.

Chaffey, D. (2023). Global social media statistics research summary 2022 [June 2022]. Smart Insights.

Cuesta, I., Montesó-Curto, P., Metzler Sawin, E., Jiménez-Herrera, M., Puig-Llobet, M., Seabra, P., & Toussaint, L. (2021). Risk factors for teen suicide and bullying: An international integrative review. *International journal of nursing practice*, *27*(3), e12930.

Donalds, C., & Osei-Bryson, K. M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, *92*, 403-418

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials*, *16*(4), 2019-2036.

Holfeld, B., & Leadbeater, B. J. (2018). The interrelated effects of traditional and cybervictimization on the development of internalizing symptoms and aggressive behaviors in elementary school. *Merrill-Palmer Quarterly*, *64*(2), 220-247.

Kowalski, R. M., & Limber, S. P. (2013). Psychological, physical, and academic correlates of cyberbullying and traditional bullying. *Journal of adolescent health*, *53*(1), S13-S20.

Kross, E., Verduyn, P., Sheppes, G., Costello, C. K., Jonides, J., & Ybarra, O. (2021). Social media and well-being: Pitfalls, progress, and next steps. *Trends in cognitive sciences*, *25*(1), 55-66.

Li, J., & Hesketh, T. (2021). Experiences and perspectives of traditional bullying and cyberbullying among adolescents in Mainland China-implications for policy. *Frontiers in psychology*, *12*, 672223.

Longobardi, C., Settanni, M., Fabris, M. A., & Marengo, D. (2020). Follow or be followed: Exploring the links between Instagram popularity, social media addiction, cyber victimization, and subjective happiness in Italian adolescents. *Children and youth services review*, *113*, 104955.

Maftei, A., & Măirean, C. (2023). Not so funny after all! Humor, parents, peers, and their link with cyberbullying experiences. *Computers in Human Behavior*, *138*, 107448.

Merlici, I. A., Maftei, A., Corlătianu, M., Lăzărescu, G., Dănilă, O., & Măirean, C. (2023). I'm doing the right thing! Technological intimate partner violence and social media use: the moderating role of moral absolutism and the mediating role of jealousy. *Ethics & Behavior*, *33*(6), 490-504.

Mesch, G. S. (2009). Parental mediation, online activities, and cyberbullying. *Cyberpsychology & behavior*, *12*(4), 387-393.

Meshi, D., Cotten, S. R., & Bender, A. R. (2020). Problematic social media use and perceived social isolation in older adults: a cross-sectional study. *Gerontology*, *66*(2), 160-168.

Munir, A., & Shabir, G. (2018). Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation. *Global Political Review (GPR)*, *3*, 84-97.

Özer, G., & Escartín, J. (2023). The making and breaking of workplace bullying perpetration: A systematic review on the antecedents, moderators, mediators, outcomes of perpetration and suggestions for organizations. *Aggression and violent behavior*, 101823

Pozzoli, T., Gini, G., & Vieno, A. (2012). The role of individual correlates and class norms in defending and passive bystanding behavior in bullying: A multilevel analysis. *Child development*, *83*(6), 1917-1931.

Tao, S., Reichert, F., Law, N., & Rao, N. (2022). Digital technology use and cyberbullying among primary school children: Digital literacy and parental mediation as moderators. *Cyberpsychology, Behavior, and Social Networking*, *25*(9), 571-579.

Umeugo, W. (2023). Cybercrime Awareness on Social Media: A Comparison Study. *International Journal of Network Security & Its Applications*, *15*(2), 23-35.

Wang, L., & Ngai, S. S. Y. (2022). Cyberbullying perpetration among Chinese adolescents: the role of power imbalance, fun-seeking tendency, and attitude toward cyberbullying. *Journal of interpersonal violence*, *37*(23-24), NP21646-NP21671

Wang, L., & Ngai, S. S. Y. (2022). Cyberbullying perpetration among Chinese adolescents: the role of power imbalance, fun-seeking tendency, and attitude toward cyberbullying. *Journal of interpersonal violence*, *37*(23-24), NP21646-NP21671.

Wheatley, D., & Buglass, S. L. (2019). Social network engagement and subjective well-being: a life-course perspective. *The British Journal of Sociology*, *70*(5), 1971-1995.

Wuryanningsih, E. W., Kurniyawan, E. H., & Cahya Aisyah, E. (2019). Correlation between emotional peer support and cyberbullying behaviour in senior high school students.

Yar, M. (2013). Cybercrime and society. *Cybercrime and Society*, 1-232.

Yassein, M. B., Aljawarneh, S., & Wahsheh, Y. A. (2019, April). Survey of online social networks threats and solutions. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)* (pp. 375-380). IEEE.

Ybarra, M. L., & Mitchell, K. J. (2004). Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of child Psychology and Psychiatry*, *45*(7), 1308-1316.

Zhang, C., Sun, J., Zhu, X., & Fang, Y. (2010). Privacy and security for online social networks: challenges and opportunities. *IEEE network*, *24*(4), 13-18.